

Japan Patent Office,
Unexamined Patent Application Publication No. 2000-99476
PUBLICATION DATE: April 7, 2000

[0010] In the present invention, when a client program acquiring request is sent from a client computer, a server computer automatically sends to a Firewall computer a skeleton object program of a server program and a stub object program of a client program of a client program as a relay program, so that the client server automatically establishes a relay program on the Firewall computer.

[0019] A browser program 12A on a client computer 1 sends a client program acquiring request to a program acquiring relay program 32A on a Firewall computer 3 (201).

[0020] In accordance with an instruction from browser program 12A, program acquiring relay program 32A relays a client program acquiring request to a program transmission server program 22A on a server computer 2 storing the destination client program (202).

[0021] Program transmission server program 22A refers to a program configuration management file 22G to determine a client object program 22D, a stub object program 22E, a skeleton object program 22C, all of which is to be transmitted (203).

[0022] Along with client object program 22D, stub object program 22E, and skeleton object program 22C, program transmission server program 22A extracts an access control file 22F from an external memory device 22, and transmits them to a program acquiring relay program 32A on a Firewall computer 3 (204).

[0023] Program acquiring relay program 32A stores skeleton object program 22C, stub object program 22E, and access control file 22F transmitted from program transmission server program 22A in an external memory device 32 (205).

[0024] Program acquiring relay program 32A sends stub object program 22E and client object program 22D back to a browser program 12A of a client computer 1 (206).

[0025] Browser program 12 A activates client object program 22D and calls stub object program 22E' when client object program 22D' request a communication with

server object program 22B (207).

[0026] Stub object program 22E' calls skeleton object program 22C' on Firewall computer 3 by attaching user verification information (user name and password) to the skeleton object program (208).

[0027] Skeleton object program 22C' on Firewall computer 3 passes user verification information to communication relay between distributed objects control program 32B, so that the communication relay between distributed objects control program checks the contents of an access control file 22F (209). The skeleton object program acquires the checked result (210).

[0028] As a result of checking, when a user is not entitled to access server object program 22, the skeleton object program replies a message indicating that the access is not permitted to stub object program 22E' of client computer 1 (215).

[0029] When the user is entitled to access server object program 22, the skeleton object program calls stub object program 22E' in Firewall computer 3 (211).

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-99476

(P 2000-99476A)

(43) 公開日 平成12年4月7日(2000.4.7)

(51) Int. Cl. ⁷

G06F 15/16

識別記号

620

F I

G06F 15/16

620

ターマコード (参考)

T 5B045

審査請求 未請求 請求項の数4 O L (全9頁)

(21) 出願番号

特願平10-262614

(22) 出願日

平成10年9月17日(1998.9.17)

(71) 出願人 000233055

日立ソフトウェアエンジニアリング株式会
社

神奈川県横浜市中区尾上町6丁目81番地

(72) 発明者 藤岡 秀樹

神奈川県横浜市中区尾上町6丁目81番地

日立ソフトウェアエンジニアリング株式会
社内

(74) 代理人 100083552

弁理士 秋田 収喜

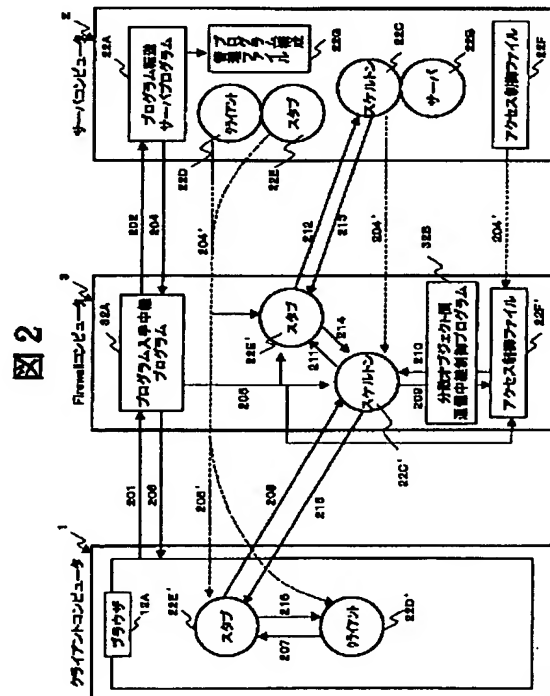
Fターム(参考) 5B045 BB31 GG01 HH02

(54) 【発明の名称】 分散オブジェクト間通信中継システム

(57) 【要約】

【課題】 Firewallコンピュータ上にサーバプログラム
への中継用のプログラムが常時稼働していることによる
メモリ、CPUの無駄な消費を防ぐこと、サーバプログ
ラムに対しアクセスが許可されていないユーザからサー
バプログラムへの通信を中継せず、無駄な通信を削減す
ること。

【解決手段】 クライアントコンピュータからサーバコ
ンピュータにクライアントプログラム入手要求があった
時点で、サーバコンピュータからサーバプログラムのス
ケルトンオブジェクトプログラムとクライアントプログ
ラムのスタブオブジェクトプログラムを中継プログラム
として、Firewallコンピュータに自動的に送信してFire
wallコンピュータ上に中継プログラムを自動的に構築す
る。



【特許請求の範囲】

【請求項 1】 ネットワーク上に分散して存在する複数のクライアントコンピュータが使用するクライアントプログラムを、ネットワークおよび所定のセキュリティシステムを中継してサーバコンピュータから取得して実行するシステムにおいて、

前記セキュリティシステム上で稼働する分散オブジェクト間通信を中継する中継プログラムを、クライアントコンピュータがサーバコンピュータからクライアントプログラムを入手する時に、サーバコンピュータから前記セキュリティシステムのコンピュータに送信して自動的に構築することを特徴とする分散オブジェクト間通信中継システム。

【請求項 2】 前記中継プログラムは、前記クライアントプログラムを構成するクライアントオブジェクトプログラムと分散オブジェクト間通信を行うためのスタブオブジェクトプログラムのうちのスタブオブジェクトと、前記サーバプログラムを構成するサーバオブジェクトプログラムと分散オブジェクト間通信を行うためのスケルトンオブジェクトのうちのスケルトンオブジェクトプログラムとから成ることを特徴とする請求項 1 記載の分散オブジェクト間通信中継システム。

【請求項 3】 前記中継プログラムを構成するスタブオブジェクトプログラムとスケルトンオブジェクトプログラムに加え、サーバオブジェクトプログラムへのアクセス可否の情報が設定されたアクセス制御情報を前記セキュリティシステムのコンピュータに送信することを特徴とする請求項 2 記載の分散オブジェクト間通信中継システム。

【請求項 4】 前記セキュリティシステムのコンピュータ上で稼働状態となったスケルトンオブジェクトプログラムは、クライアントプログラム内のスタブオブジェクトプログラムからの通信を受信した時に、クライアントコンピュータのアドレス、スタブオブジェクトプログラムの識別子、スタブオブジェクトプログラムの利用者識別子のうち少なくとも 1 つを認識し、サーバオブジェクトプログラムを使用可能かどうかを前記アクセス制御情報に基づいて判定し、使用不可の場合には、サーバプログラムのスケルトンオブジェクトプログラムに対して中継を行わないことを特徴とする請求項 3 記載の分散オブジェクト間通信中継システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、インターネットやイントラネットなどの様々なネットワーク上に存在するクライアントコンピュータが、サーバコンピュータからクライアントプログラムを入手し、サーバコンピュータで稼働するサーバオブジェクトプログラムとの間で分散オブジェクト通信技術を使用して通信を行う際に、Firewall コンピュータなどによって物理的にネットワークが

分離されている場合に、Firewall コンピュータ上で分散オブジェクト間通信を中継する中継プログラムを、クライアントコンピュータがクライアントプログラムを入手する時に自動的に構築（インストール）し、その中継プログラムがサーバオブジェクトプログラムへのアクセス制御を行うことで、Firewall コンピュータとサーバコンピュータ間の通信量を削減するために適用して有効な分散オブジェクト間通信の中継技術に関するものである。

【0002】

【従来の技術】 WWW (World Wide Web) サービスの発展によって、WWW ブラウザを使用してサーバアプリケーションにアクセスして情報を入手するプログラムが実現され、遠隔地から Firewall (不正アクセスを防ぐための防火壁と呼ばれるセキュリティシステム) によって分離されたサーバコンピュータ上のプログラムに通信できる環境が整ってきている。

【0003】 例えば、WWW ブラウザ上で見ることができる HTML (Hyper Text Markup Language) ファイルを WWW サーバから入手するための通信プロトコルである HTTP (Hyper Text Transfer Protocol) を中継するためのものとして、電子総合技術研究所の佐藤豊氏が開発した「delegate」がある。「delegate」は、HTTP だけでなく FTP (File Transfer Protocol) や NNTP (Network News Transfer Protocol), SMTP (Simple Mail Transfer Protocol) などのインターネットで標準的に使われるプロトコルの中継を行うプログラムである。これは、Firewall コンピュータ上で稼働し、クライアントコンピュータからサーバコンピュータを指定した通信を一旦受信し、指定されたサーバコンピュータに接続してクライアントコンピュータからの要求をサーバアプリケーションに中継し、サーバアプリケーションからの結果を受信してクライアントプログラムに返却するというものである。

【0004】 また、米国 Borland 社の ORB 製品である Visibroker は CORBA 準拠製品であり、CORBA の通信プロトコルである IIOP を中継する Gatekeeper というプログラムを提供している。これによって、クライアントプログラムから分散オブジェクト間通信を利用してサーバコンピュータに接続しようとした場合に、一旦 Gatekeeper プログラムが通信を受信して、通信対象であるサーバアプリケーションのスケルトンオブジェクトとの通信を可能としている。

【0005】 以上で説明したプログラムは、Firewall 上で稼働するプログラムであり、クライアントプログラムからサーバプログラムへの接続可否に関わらず常時稼働しており、どのクライアントコンピュータからどのサーバコンピュータにアクセスできるかを管理する機能は提供している。

【0006】

【発明が解決しようとする課題】 しかしながら、上記従

来技術にあっては、Firewallコンピュータ上に中継用のプログラムが常時稼働状態で待機しているため、メモリ、CPUが無駄に消費されているという問題がある。

【0007】また、クライアントプログラムとサーバプログラム間の分散オブジェクト間通信を中継する際には、中継プログラムは接続して来たクライアントアプリケーションのスタブオブジェクトや、サーバアプリケーションのスケルトンオブジェクトの内容を全く知らずに、ただ通信されるデータの中継するだけである。そのため、サーバプログラムを利用することが許可されていないユーザがクライアントコンピュータからアクセスしてきても、一旦サーバプログラムへデータを中継して、サーバプログラムがアクセスを拒否した結果をクライアントコンピュータに通信しなければならない。したがって、サーバプログラムを利用することが許可されていないユーザがサーバプログラムに対してアクセスした場合には、無駄な通信と中継処理が行われることになってしまうという問題がある。

【0008】本発明の第1の目的は、Firewallコンピュータ上にサーバプログラムへの中継用のプログラムが常時稼働していることによるメモリ、CPUの無駄な消費を防ぐことが可能な分散オブジェクト間中継システムを提供することである。

【0009】本発明の第2の目的は、サーバプログラムに対しアクセスが許可されていないユーザからサーバプログラムへの通信を中継せず、無駄な通信を削減することが可能な分散オブジェクト間中継システムを提供することである。

【0010】

【課題を解決するための手段】本発明は、上記目的を達成するために、クライアントコンピュータからサーバコンピュータにクライアントプログラム入手要求があった時点で、サーバコンピュータからサーバプログラムのスケルトンオブジェクトプログラムとクライアントプログラムのスタブオブジェクトプログラムを中継プログラムとして、Firewallコンピュータに自動的に送信してFirewallコンピュータ上に中継プログラムを自動的に構築するようにしたものである。

【0011】また、スケルトンオブジェクトプログラムとスタブオブジェクトプログラムとから成る中継プログラムを送信する際に、サーバオブジェクトプログラムへのアクセス制御情報をFirewallコンピュータに自動的に送信し、そのアクセス制御情報に基づいてFirewallコンピュータ上でアクセス制御を行うようにしたものである。

【0012】

【発明の実施の形態】以下、本発明の一実施形態を図面を用いて説明する。

【0013】図1は、本発明の一実施の形態を示すシステム構成図である。

【0014】この実施形態のシステムは、大別すると、クライアントコンピュータ1と、サーバコンピュータ2と、Firewallコンピュータ3と、クライアントコンピュータ1とFirewallコンピュータ3間で送受信されるデータを通信するためのネットワーク4と、Firewallコンピュータ3とサーバコンピュータ2間で送受信されるデータを通信するためのネットワーク5とから構成されている。

【0015】クライアントコンピュータ1は、CPU11A、メモリ11Bからなる端末装置11、クライアントプログラムをサーバコンピュータ2から入手して実行するブラウザプログラム12Aが格納されている外部記憶装置12と、サーバプログラムの実行結果を表示するための表示装置13と、ブラウザプログラム12Aの起動の指示や、クライアントプログラム実行時にユーザ名称やパスワードの入力を行うための入力装置14と通信ポート15とから構成されている。

【0016】サーバコンピュータ2は、CPU21A、メモリ21Bからなる端末装置21と、クライアントコンピュータ1からのプログラム入手要求を受け付けるプログラム転送サーバプログラム22A、サーバオブジェクトプログラム22B、スケルトンオブジェクトプログラム22C、クライアントオブジェクトプログラム22D、スタブオブジェクトプログラム22E、サーバオブジェクトに対するアクセス制御情報を記述したアクセス制御ファイル22F、スタブオブジェクトプログラムとスケルトンオブジェクトプログラム、アクセス制御ファイルの対応を記述したプログラム構成管理ファイル22Gを格納されている外部記憶装置22と、通信ポート23とから構成されている。

【0017】Firewallコンピュータ3は、CPU31A、メモリ31Bからなる端末装置31と、クライアントコンピュータ1からのクライアントプログラム入手要求をサーバコンピュータ2のプログラム転送サーバプログラム22Aに中継するためのプログラム入手中継プログラム32Aと、サーバコンピュータ2からスタブオブジェクトプログラム22Eとスケルトンオブジェクトプログラム22Cを入手して実行する、分散オブジェクト間通信中継制御プログラム32Bを格納するための外部記憶装置32と、通信ポート33とから構成されている。

【0018】図2は、本実施形態のクライアントコンピュータ1、Firewallコンピュータ3、サーバコンピュータ2間でやり取りされる情報の流れと、各コンピュータ上で起動して実行されるプログラムの関連を示したものである。

【0019】まず、クライアントコンピュータ1上のブラウザプログラム12Aがクライアントプログラム入手依頼をFirewallコンピュータ3上のプログラム入手中継プログラム32Aに送信する(201)。

【0020】プログラム入手中継プログラム32Aは、ブラウザプログラム12Aからの指示にしたがって、入手したいクライアントプログラムを格納しているサーバコンピュータ2上のプログラム転送サーバプログラム22Aにクライアントプログラムの入手依頼を中継する(202)。

【0021】プログラム転送サーバプログラム22Aは、プログラム構成管理ファイル22Gを参照し、転送すべきクライアントオブジェクトプログラム22D、スタブオブジェクトプログラム22E、スケルトンオブジェクトプログラム22Cを判断する(203)。

【0022】プログラム転送サーバプログラム22Aは、外部記憶装置22からクライアントオブジェクトプログラム22D、スタブオブジェクトプログラム22E、スケルトンオブジェクトプログラム22Cに加え、アクセス制御ファイル22Fを取り出し、Firewallコンピュータ3上のプログラム入手中継プログラム32Aに返送する(204、204')。

【0023】プログラム入手中継プログラム32Aは、プログラム転送サーバプログラム22Aから送信されてきたスケルトンオブジェクトプログラム22Cとスタブオブジェクトプログラム22E、アクセス制御ファイル22Fを外部記憶装置32中に格納し、分散オブジェクト間通信中継制御プログラム32Bが、オブジェクトを生成して接続を待っている(205)。

【0024】プログラム入手中継オブジェクト32Aは、スタブオブジェクトプログラム22Eとクライアントオブジェクトプログラム22Dをクライアントコンピュータ1のブラウザプログラム12Aに返送する(206、206')。

【0025】ブラウザプログラム12Aは、クライアントオブジェクトプログラム22D'を起動し、クライアントオブジェクトプログラム22D'がサーバオブジェクトプログラム22Bと通信を必要とした時にスタブオブジェクトプログラム22E'を呼び出す(207)。

【0026】スタブオブジェクトプログラム22E'は、ネットワーク4経由でFirewallコンピュータ3上のスケルトンオブジェクトプログラム22C'に対して、ユーザ認証情報(ユーザ名とパスワードなど)を追加して呼び出す(208)。

【0027】Firewallコンピュータ3上のスケルトンオブジェクトプログラム22C'は、分散オブジェクト間通信中継制御プログラム32Bにユーザ認証情報を渡し、アクセス制御ファイル22F'の内容をチェックしてもらい(209)、チェックした結果を入手する(210)。

【0028】チェックした結果、サーバオブジェクトプログラム22Bへのアクセスが出来ないユーザであれば、アクセス拒否のメッセージをクライアントコンピュータ1のスタブオブジェクトプログラム22E'に返却

する(215)。

【0029】アクセス可能であれば、Firewallコンピュータ3内のスタブオブジェクトプログラム22E'を呼び出す(211)。

【0030】Firewallコンピュータ3内のスタブオブジェクトプログラム22E'は、ネットワーク5経由でサーバコンピュータ2上のスケルトンオブジェクトプログラム22Cを呼び出す(212)。

【0031】スケルトンオブジェクトプログラム22Cは、サーバオブジェクトプログラム22Bを実行して、結果をネットワーク5経由でFirewallコンピュータ3上のスタブオブジェクトプログラム22E'に返却する(213)。

【0032】Firewallコンピュータ3上のスタブオブジェクトプログラム22E'は、スケルトンオブジェクトプログラム22C'に結果を返却し(214)、スケルトンオブジェクトプログラム22C'は、クライアントコンピュータ1上のスタブオブジェクトプログラム22E'に値を返却する(215)。

【0033】クライアントコンピュータ1上のスタブオブジェクトプログラム22E'がクライアントオブジェクトプログラム22D'に値を返却し(216)、分散オブジェクト通信中継を使用したサーバオブジェクトプログラム22Bへの呼出しが終了する。

【0034】図3は、本実施形態のFirewallコンピュータ3上で稼働するスケルトンオブジェクトプログラム22C'がクライアントオブジェクトプログラム22D'からの接続に対してアクセス制御を行うために、サーバコンピュータ2上に格納しておくアクセス制御ファイル22Fの例を示したものである。

【0035】図示する例のアクセス制御ファイル22Fには、[USERPASS]が書かれた次の行からは、ユーザ名称301と、そのユーザのパスワードが暗号化されたもの(302)が空白(スペースまたはタブ)で区切られて1行ごとに対になって記述されている。

【0036】また、[OBJACL]が書かれた次の行からは、サーバオブジェクトプログラム22Bの名前303と、サーバオブジェクトプログラム22Bにアクセス可能なクライアントコンピュータ1のアドレス30

4、サーバオブジェクトプログラム22Bにアクセス可能なユーザ名称305が空白(スペースまたはタブ)で区切られて1行ごとに組になって記述されている。

【0037】クライアントコンピュータ1のアドレスは、IPアドレスを直に記したものや、' * 'によってIPアドレス群を記したもの、コンピュータの名称を直に記したものや、' * 'によってコンピュータ名称群を記したものが、' , 'によって区切られて記載される。

【0038】ユーザ名称は、' , 'によって区切られて記載される。また、' * 'の場合は全てのユーザがアクセス可能なことを示す。

【0039】図4は、サーバコンピュータ2上で稼働するプログラム転送サーバプログラム22Aが、クライアントコンピュータ1に転送するクライアントオブジェクトプログラム22Dとスタブオブジェクトプログラム22Eに対応して、Firewallコンピュータ3に転送するスケルトンオブジェクトプログラム22Cと、サーバオブジェクトプログラム22Bに対するアクセス制御情報を記述したアクセス制御ファイルの関連を記述するプログラム構成管理ファイル22Gの例を示したものである。

【0040】図示する例のプログラム構成管理ファイル22Gには、クライアントオブジェクトプログラム22Dの名称401、スタブオブジェクトプログラム22Eの名称402、それに対応するスケルトンオブジェクトプログラム22Cの名称403と、そのスケルトンオブジェクトプログラム22Cからアクセスされるサーバオブジェクトプログラムに関するアクセス制御情報が記載されているアクセス制御ファイル22Fの名称404が、空白（スペースまたはタブ）で区切られて1行ごとに組になって記載されている。

【0041】以下、フローチャートを用いて、本実施形態の動作を説明する。

【0042】図5は、本実施例のクライアントコンピュータ1上で稼働するブラウザプログラム12Aの動作を示すフローチャートである。

【0043】ブラウザプログラム12Aが起動すると、入力装置14からクライアントオブジェクトプログラム22Dの名称とクライアントオブジェクトプログラム22Dが格納されているサーバコンピュータ2の名称を受け付ける（ステップ501）。

【0044】次に、Firewallコンピュータ3のプログラム入手中継プログラム32Aに接続し、ステップ501で入手したサーバコンピュータ2の名称とクライアントオブジェクトプログラム22Dの名称を送信する（ステップ502）。

【0045】その結果として、プログラム入手中継プログラム32Aからクライアントオブジェクトプログラム22D'とスタブオブジェクトプログラム22E'を受信する（ステップ503）。

【0046】次に、受信したクライアントオブジェクトプログラム22D'を起動し（ステップ504）、スタブオブジェクトプログラム22E'経由でFirewallコンピュータ3上のスケルトンオブジェクトプログラム22C'にユーザ名称とパスワードを送信し、その結果としてサーバオブジェクトプログラム22Bにアクセス可能かどうかの認証結果を受信する（ステップ505）。

【0047】受信した結果がサーバオブジェクトプログラム22Bにアクセス可能かどうかを判断し（ステップ506）、アクセス不可能であった場合はクライアントオブジェクトプログラム22D'を終了し（ステップ507）、さらにブラウザプログラム12Aを終了する。

【0048】ステップ506の結果がアクセス可能であった場合は、スタブオブジェクトプログラム22E'経由でサーバオブジェクトプログラム22Bを呼び出し（ステップ508）、結果をスタブオブジェクトプログラム22E'から受け取って表示装置13の画面に表示する（ステップ509）。その後、クライアントオブジェクトプログラム終了の指示を受けるまで、ステップ508からの処理を繰り返す。

【0049】図6は、サーバコンピュータ3上で稼働するプログラム転送サーバプログラム22Aの動作を示すフローチャートである。

【0050】プログラム転送サーバプログラム22Aが起動すると、Firewallコンピュータ3上で稼働しているプログラム入手中継プログラム32Aからの接続を受け（ステップ601）、入手したいクライアントオブジェクトプログラム22Dの名称を受信する（ステップ602）。その後、図4に示したプログラム構成管理ファイル22Gからクライアントオブジェクトプログラム22Dと同時に転送すべきスタブオブジェクトプログラム22Eとスケルトンオブジェクトプログラム22C、アクセス制御ファイル22Fの名称を入手し（ステップ603）、プログラム入手中継プログラム32Aへ転送し（ステップ604）、ステップ601から繰り返す。

【0051】図7は、Firewallコンピュータ3上で稼働するプログラム入手中継プログラム32Aの動作を示すフローチャートである。

【0052】プログラム入手中継プログラム32Aが起動すると、クライアントコンピュータ1上で稼働しているブラウザプログラム12Aから接続を受け（ステップ701）、ブラウザプログラム12Aが入手したいクライアントオブジェクトプログラム22Dの名称を受信する（ステップ702）。次に、サーバコンピュータ3上で稼働しているプログラム転送サーバプログラム22Aに接続し、先ほど受信したクライアントオブジェクトプログラム22Dの名称を送信する（ステップ703）。その結果として、プログラム転送サーバプログラム22Aから、クライアントオブジェクトプログラム22D'、スタブオブジェクトプログラム22E'、スケルトンオブジェクトプログラム22C'、アクセス制御ファイル22F'を受信する（ステップ704）。

【0053】受信したオブジェクトプログラムのうち、スタブオブジェクトプログラム22E'、スケルトンオブジェクトプログラム22C'、アクセス制御ファイル22F'は、外部記憶装置32中に格納し（ステップ705）、分散オブジェクト間通信中継制御プログラム32Bにスケルトンオブジェクトプログラム22C'とスタブオブジェクトプログラム22E'、アクセス制御ファイル22F'を入手したことを通知する（ステップ706）。その後、クライアントオブジェクトプログラム22D'とスタブオブジェクトプログラム22E'を

ラウザプログラム 12A に転送し (ステップ 707)、ステップ 701 から繰り返す。

【0054】図 8 は、Firewall コンピュータ上で稼動する分散オブジェクト間通信中継制御プログラム 32B の動作を示すフローチャートである。

【0055】分散オブジェクト間通信中継制御プログラム 32B が起動すると、プログラム入手中継プログラム 32A またはスタブオブジェクトプログラム 22E からの接続を待つ (ステップ 801)。プログラム入手中継プログラム 32A からの接続かどうかを判断し (ステッ

プ 802)、そうであれば、スケルトンオブジェクトプログラム 22C' とスタブオブジェクトプログラム 22E'、アクセス制御ファイル 22F' の名称を受信し (ステップ 803)、外部記憶装置 32 に格納された対応するプログラムを起動して (ステップ 804)、ステップ 801 から繰り返す。スタブオブジェクトプログラム 22E' からの接続の場合には、クライアントコンピュータ 1 のアドレス、ユーザ名称、パスワードを受信し (ステップ 805)、アクセス制御ファイル 22F' を読み込んでサーバオブジェクトプログラム 22B へのア

クセスが可能かどうかを調べる (ステップ 806)。

【0056】次に、調べた結果を YES/NO という値でクライアントコンピュータ上のスケルトンオブジェクトプログラム 22E' に送信し (ステップ 807)、ステップ 801 から繰り返す。

【0057】以上のように、本実施形態のシステムにおいては、サーバコンピュータ 2 上に、サーバプログラムを構成するサーバオブジェクトプログラム 22B とスケルトンオブジェクトプログラム 22C、クライアントプログラムを構成するクライアントオブジェクトプログラム 22D とスタブオブジェクトプログラム 22E、サーバオブジェクトへのアクセス可否を設定するアクセス制御ファイル 22F を用意し、クライアントコンピュータ 1 からサーバコンピュータ 2 に対してクライアントプログラム入手の要求が Firewall コンピュータ 3 を経由して行われた時に、クライアントコンピュータ 1 にクライアントオブジェクトプログラム 22D とスタブオブジェクトプログラム 22E を転送する際に、Firewall コンピュータ 3 上にスタブオブジェクトプログラム 22E と、スケルトンオブジェクトプログラム 22C をインストール

する。さらに、サーバプログラム 2 へのアクセス可否を設定したアクセス制御ファイル 22F も同時に転送しておく。

【0058】そして、クライアントコンピュータ 1 がクライアントオブジェクトプログラム 22D' の実行を始め、分散オブジェクト間通信を使用してクライアントオブジェクトプログラム 22D' からサーバオブジェクトプログラム 22B のオブジェクトを呼び出す時に、クライアントコンピュータ 1 上のスタブオブジェクトプログラム 22E' が Firewall コンピュータ 3 上のスケルトン

オブジェクトプログラム 22C' を呼び出し、そのスケルトンオブジェクトプログラム 22C' によって、呼出し時に渡されたユーザ名とパスワードなどのユーザを指定する情報や、マシンのアドレスなどの情報を使用して、アクセス制御ファイル 22F' の内容と比較することでサーバオブジェクトプログラム 22B にアクセス可能かどうかを判断し、アクセス可能な場合は、Firewall コンピュータ 3 上のスタブオブジェクトプログラム 22E' を使って、サーバコンピュータ 2 上のサーバオブジェクトプログラム 22B 中のスケルトンオブジェクト 22C を呼び出して、サーバオブジェクトプログラム 22B を実行する。サーバオブジェクトプログラム 22B の実行結果は、Firewall コンピュータ 3 上のスタブオブジェクトプログラム 22E'、スケルトンオブジェクトプログラム 22C'、クライアントコンピュータ 1 上のスタブオブジェクトプログラム 22E' を経由して、クライアントオブジェクトプログラム 22D' に返される。

【0059】Firewall コンピュータ 3 のスタブオブジェクトプログラム 22E' によって、サーバオブジェクトプログラム 22B に対してアクセスできないと判断された場合には、この時点でアクセス拒否のメッセージをクライアントコンピュータ 1 上のスタブオブジェクトプログラム 22E' を経由してクライアントオブジェクトプログラム 22D' に返却する。

【0060】このような構成にすることにより、Firewall コンピュータ 3 上に分散オブジェクト間通信の中継するプログラム (スタブオブジェクトプログラム 22E' とスケルトンオブジェクトプログラム 22C') を事前に設定して常時稼働させておく必要はなく、また、クライアントコンピュータ 1 がサーバオブジェクトプログラム 22B にアクセスできない場合に、Firewall コンピュータ 3 からサーバコンピュータ 2 への通信を発生させずに済み、不要な通信を削減し、トラフィックの増加を防止することができる。

【0061】この場合、Firewall コンピュータ 3 上には、プログラム入手中継プログラム 32A が常時稼働しているのであるが、このプログラム入手中継プログラム 32A はクライアントコンピュータ 1 からクライアントオブジェクトプログラム 22D の入手要求があった時に、オブジェクトプログラムファイルの転送処理だけを行うものであり、プログラム実行時の通信の中継処理を行うものではないから、常駐による CPU 資源の消費は分散オブジェクトの汎用的な中継プログラムに比べて極めて小さく、CPU 資源の無駄な消費を削減できるのである。

【0062】また、サーバオブジェクトプログラム 22B に対しアクセスが許可されていないユーザの場合、サーバコンピュータ間の通信が 1 回行われ、クライアントオブジェクトプログラムを入手できるが、その後の Firewall コンピュータ 3 内におけるユーザ認証によってアク

セスが許可されないため、クライアントコンピュータ 1 とサーバコンピュータ 2 との間の無駄な通信はなくなる。この場合、中継プログラムが既に構築されている状態で、アクセス権限のないユーザがアクセスを行おうとした場合には、Firewallコンピュータ 3 のアクセス制御によって直ちに拒否される。

【0063】なお、Firewallコンピュータ 3 内にインストールされた中継プログラムは、クライアントコンピュータ 1 上のクライアントオブジェクトプログラム 22 D' が処理を終了し、スタブオブジェクト 22 E' が、Firewallコンピュータ 3 上のスケルトンオブジェクトプログラム 22 C' との接続を切断した時点でメモリ中からアンインストールされる。

【0064】

【発明の効果】以上説明したように本発明によれば、Firewallコンピュータ上にサーバプログラムへの中継用のプログラムが常時稼働していることによるメモリ、CPU の無駄な消費を防ぐことができる。

【0065】また、サーバプログラムに対しアクセスが許可されていないユーザからサーバプログラムへの通信を中継せず、無駄な通信を削減することができる。

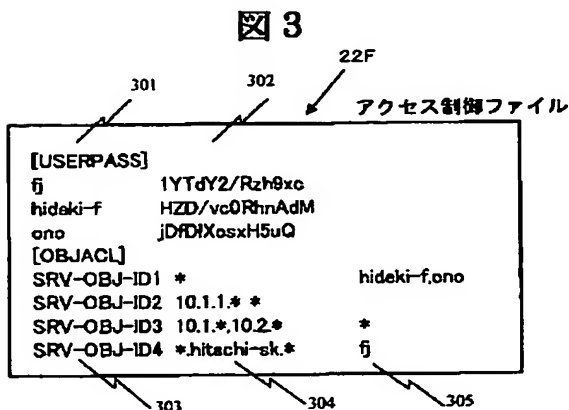
【図面の簡単な説明】

【図 1】本発明に係る分散オブジェクト間通信中継を使用した分散サービスシステムのブロック構成図である。

【図 2】本発明に係るクライアントコンピュータ、Firewallコンピュータ、サーバコンピュータ間でやり取りされる情報の流れと、各コンピュータ上で起動して実行されるプログラムの関係の例を示す図である。

【図 3】本発明に係るFirewallコンピュータ上で稼働するスケルトンオブジェクトプログラムがクライアントプログラムからの接続に対してアクセス制御を行うために、サーバコンピュータ上に格納しておくアクセス制御情報の例を示す図である。

【図 3】



【図 4】本発明に係るサーバコンピュータ上に格納されているプログラム構成管理ファイルの例を示す図である。

【図 5】本発明に係るクライアントコンピュータ上で稼働するブラウザプログラムの動作を示すフローチャートである。

【図 6】本発明に係るサーバコンピュータ上で稼働するプログラム転送サーバプログラムの動作を示すフローチャートである。

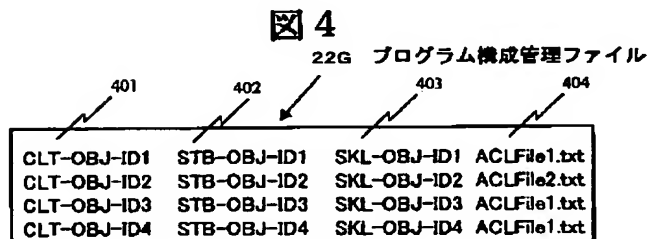
【図 7】本発明に係るFirewallコンピュータ上で稼働するプログラム入手中継プログラムの動作を示すフローチャートである。

【図 8】本発明に係るFirewallコンピュータ上で稼働する分散オブジェクト間通信中継制御プログラムの動作を示すフローチャートである。

【符号の説明】

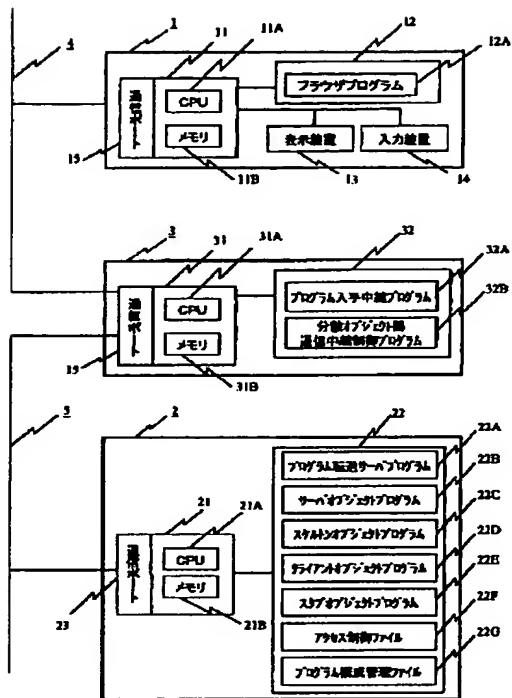
1…クライアントコンピュータ 1、2…サーバコンピュータ、3…Firewallコンピュータ、4、5…ネットワーク、11…端末装置、11A…CPU、11B…メモリ、12…外部記憶装置、12A…ブラウザプログラム 12A、13…表示装置、14…入力装置、15…通信ポート、21…端末装置、21A…CPU、21B…メモリ、22…外部記憶装置、22A…プログラム転送サーバプログラム、22B…サーバオブジェクトプログラム、22C…スケルトンオブジェクトプログラム、22D…クライアントオブジェクトプログラム、22E…スタブオブジェクトプログラム、22F…アクセス制御ファイル、22G…プログラム構成管理ファイル、23…通信ポート、31…端末装置、31A…CPU、31B…メモリ、32…外部記憶装置、32A…プログラム入手中継プログラム、32B…分散オブジェクト間通信中継制御プログラム、33…通信ポート。

【図 4】



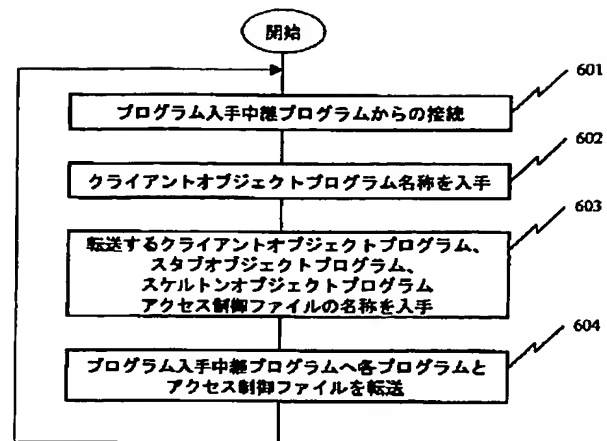
【図 1】

図 1



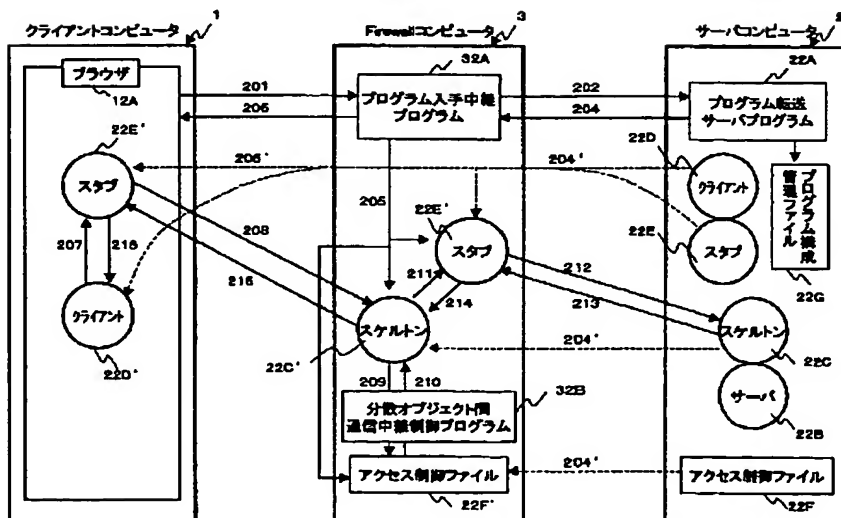
【図 6】

図 6

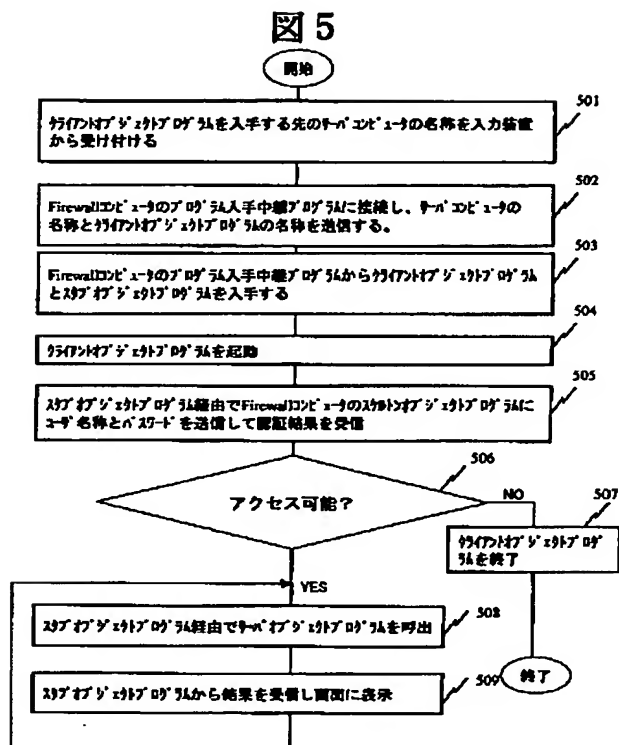


【図 2】

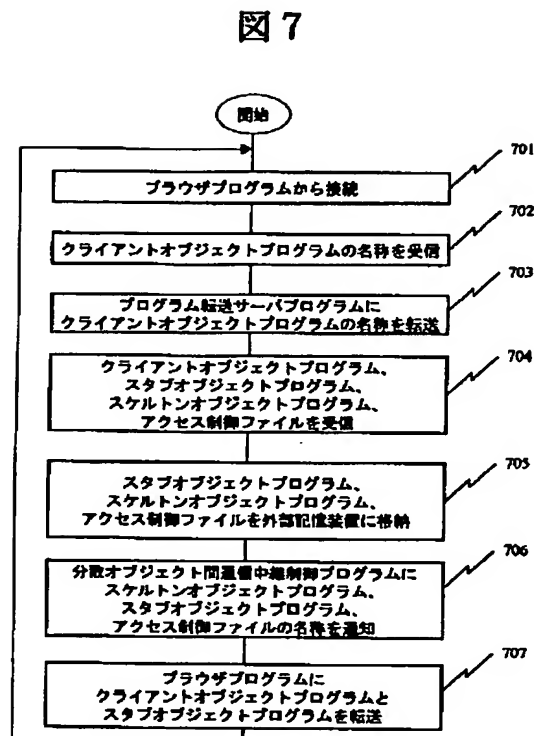
図 2



【図 5】



【図 7】



【図 8】

図 8

